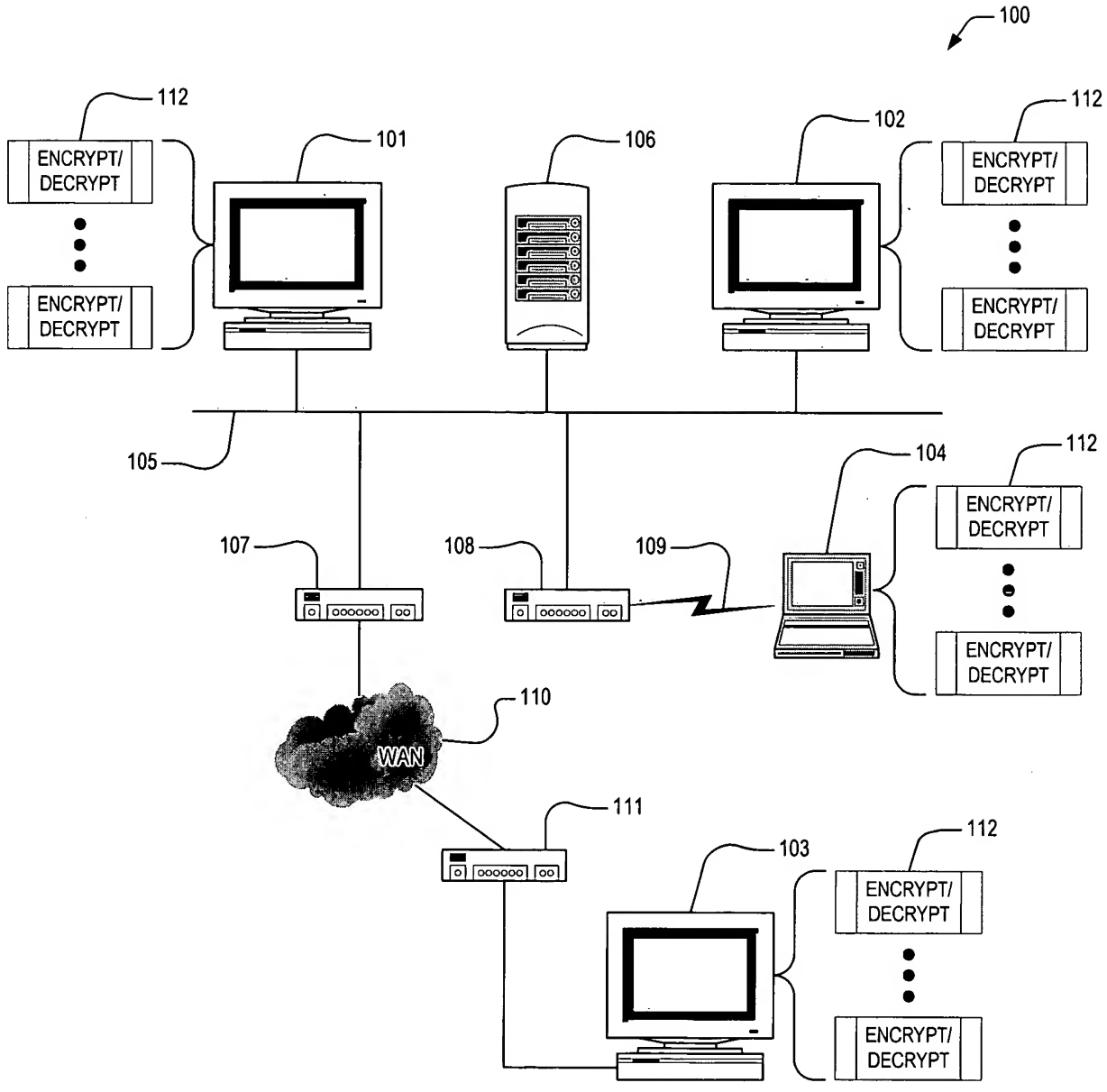
100
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
101
106
102
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
105
104
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT
107
108
109
110
WAN
111
103
112
ENCRYPT/
DECRYPT
ENCRYPT/
DECRYPT

FIG. 1

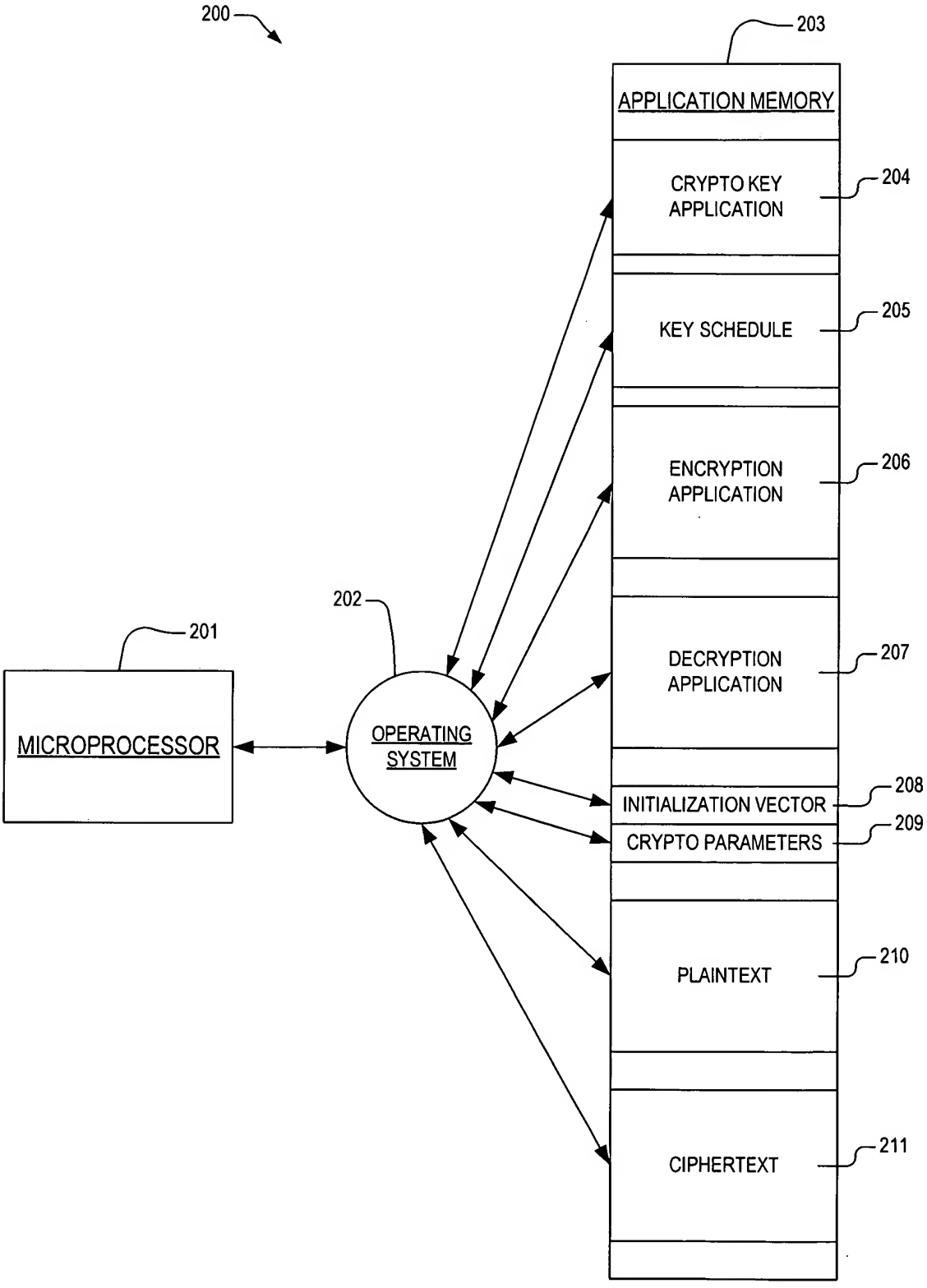
200
203
APPLICATION MEMORY
CRYPTO KEY APPLICATION
204
KEY SCHEDULE
205
ENCRYPTION APPLICATION
206
DECRYPTION APPLICATION
207
INITIALIZATION VECTOR
208
CRYPTO PARAMETERS
209
PLAINTEXT
210
CIPHERTEXT
211
202
OPERATING SYSTEM
201
MICROPROCESSOR

FIG. 2

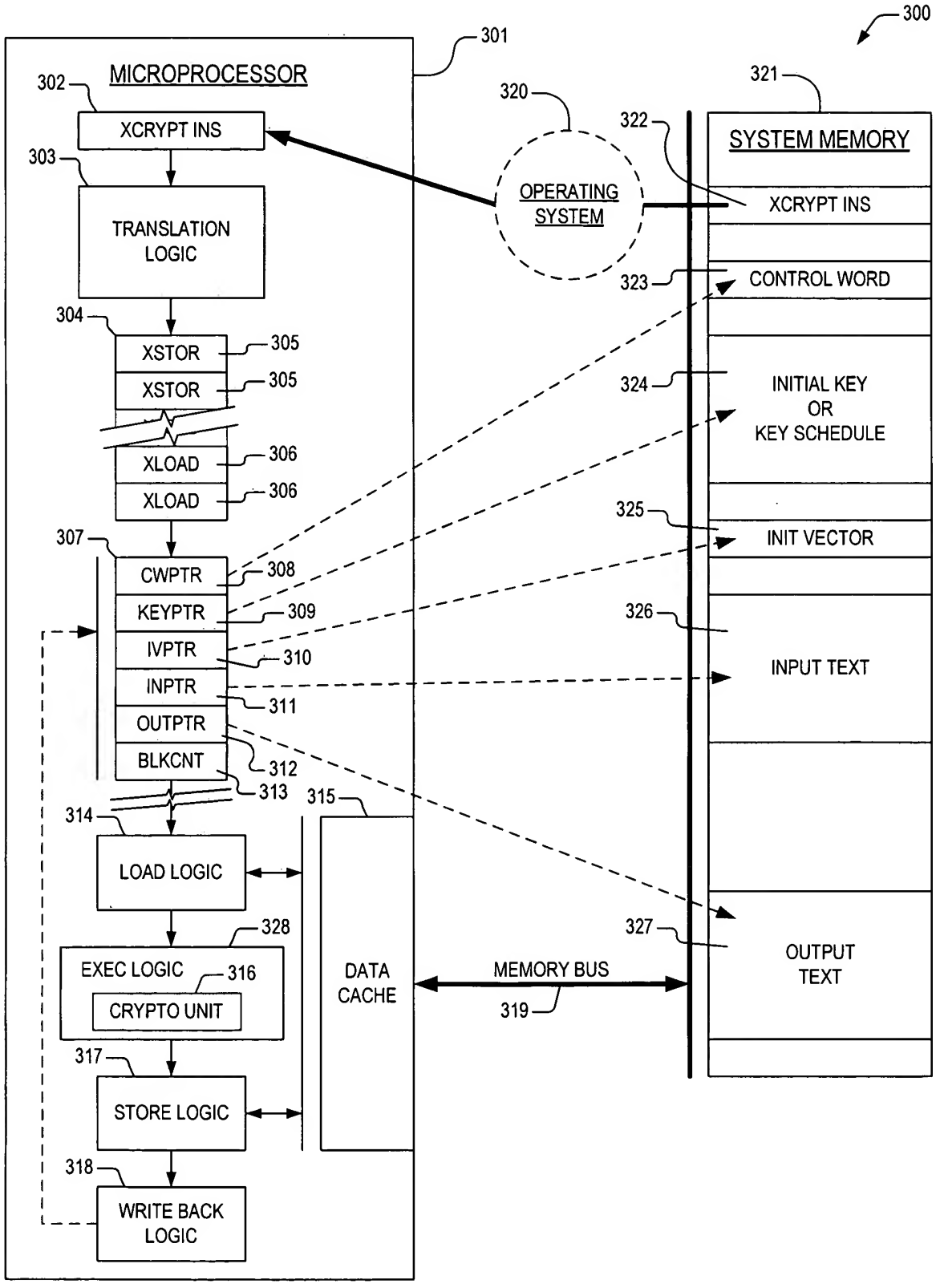
300
301
MICROPROCESSOR
302
XCRYPT INS
303
TRANSLATION LOGIC
304
XSTOR
305
XSTOR
305
XLOAD
306
XLOAD
306
307
CWPTR
308
KEYPTR
309
IVPTR
310
INPTR
311
OUTPTR
BLKCNT
312
313
314
LOAD LOGIC
315
328
EXEC LOGIC
316
CRYPTO UNIT
317
STORE LOGIC
318
WRITE BACK LOGIC
DATA CACHE
320
OPERATING SYSTEM
321
SYSTEM MEMORY
322
XCRYPT INS
323
CONTROL WORD
324
INITIAL KEY OR KEY SCHEDULE
325
INIT VECTOR
326
INPUT TEXT
327
OUTPUT TEXT
MEMORY BUS
319

FIG. 3

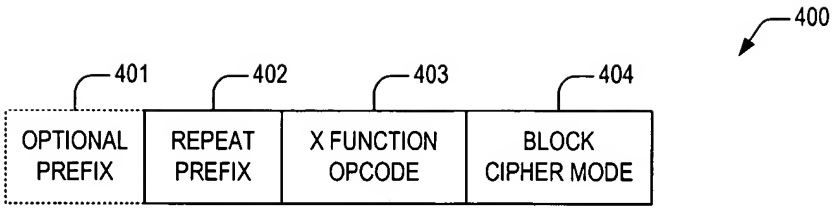

FIG. 4

500

BCM VALUE	MODE
0xC8	ELECTRONIC CODE BOOK (ECB)
0xD0	CIPHER BLOCK CHAINING (CBC)
0xE0	CIPHER FEEDBACK (CFB)
0xE8	OUTPUT FEEDBACK (OFB)
ALL OTHER VALUES	RESERVED

FIG. 5

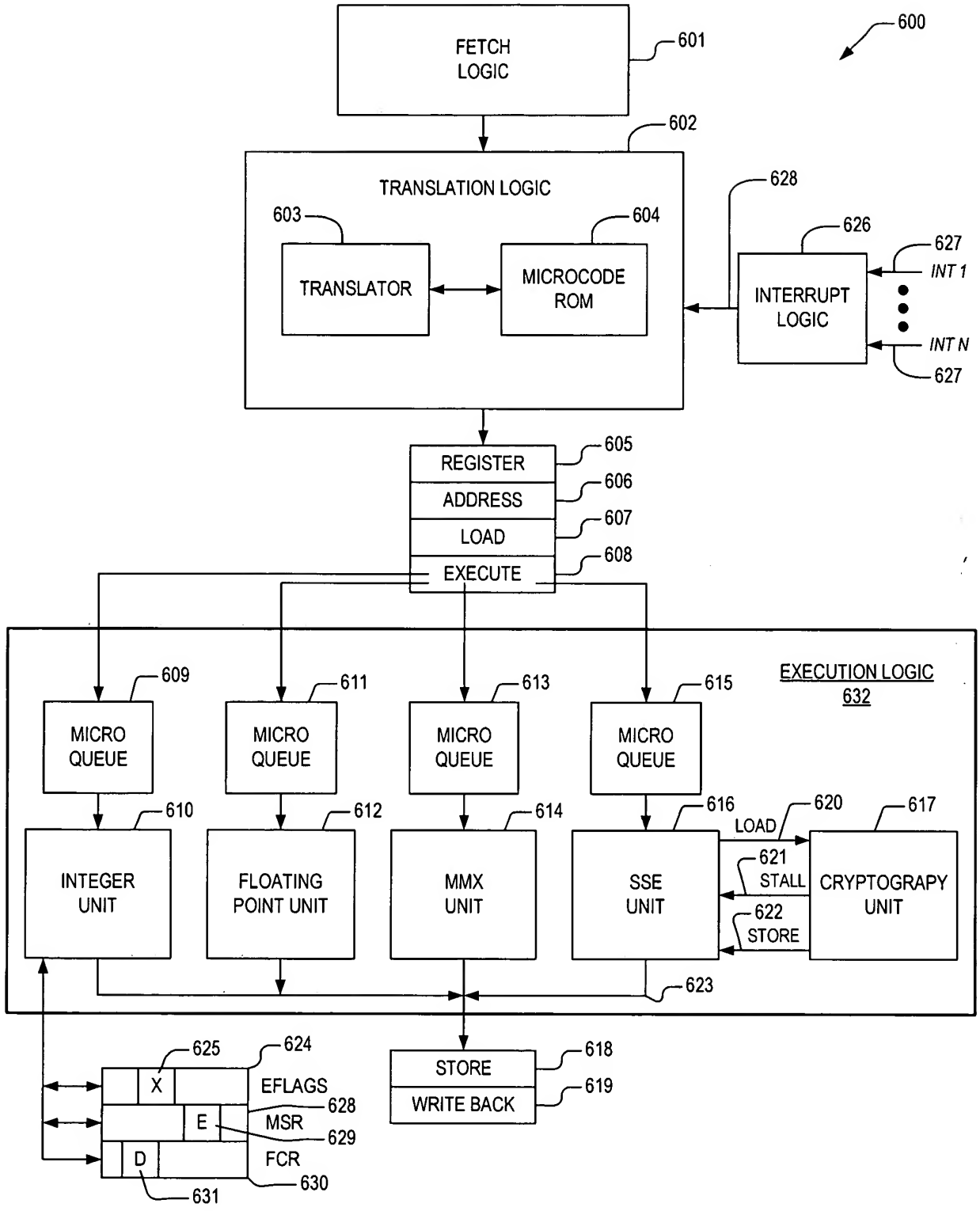
600
FETCH LOGIC
601
602
TRANSLATION LOGIC
603
TRANSLATOR
604
MICROCODE ROM
628
626
627
INT 1
INTERRUPT LOGIC
INT N
627
REGISTER
ADDRESS
LOAD
EXECUTE
605
606
607
608
EXECUTION LOGIC 632
609
611
613
615
MICRO QUEUE
MICRO QUEUE
MICRO QUEUE
MICRO QUEUE
610
612
614
616
620
617
LOAD
INTEGER UNIT
FLOATING POINT UNIT
MMX UNIT
SSE UNIT
621
STALL
622
STORE
CRYPTOGRAPY UNIT
623
625
624
X
EFLAGS
E
MSR
628
629
D
FCR
630
631
STORE
WRITE BACK
618
619

FIG. 6

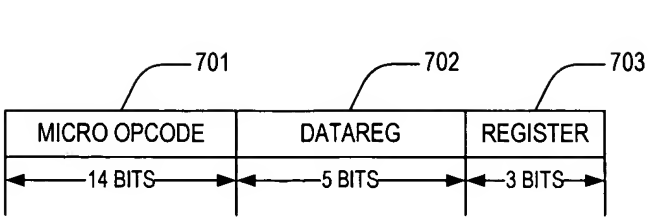

FIG. 7

800

VALUE	OPERATION
000	RESERVED
001	RESERVED
010	LOAD CONTROL WORD (CW) REGISTER
011	RESERVED
100	LOAD INPUT-0 (IN-0) REGISTER AND START CRYPTOGRAPHY UNIT
101	LOAD INPUT-1 (IN-1) REGISTER
110	LOAD CRYPTO KEY-0 REGISTER (LOWER 128 BITS OF KEY)
111	LOAD CRYPTO KEY-1 REGISTER (UPPER 128 BITS OF KEY)

FIG. 8

900

VALUE	OPERATION
000	RESERVED
001	RESERVED
010	RESERVED
011	RESERVED
100	STORE OUTPUT-0 (OUT-0) REGISTER
101	STORE OUTPUT-1 (OUT-1) REGISTER
110	RESERVED
111	RESERVED

FIG. 9

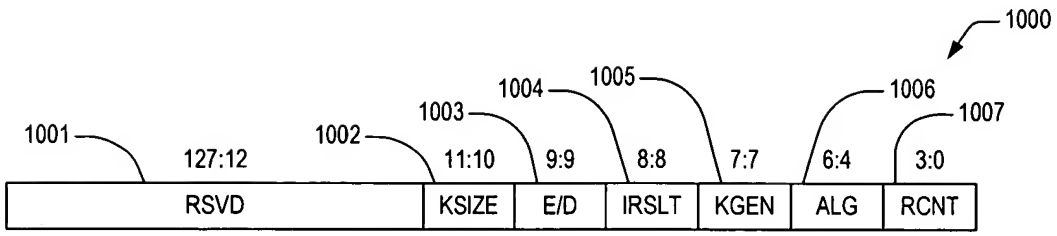

FIG. 10

1100

IRSLT VALUE	OPERATION
0	GENERATE NORMAL RESULT
1	GENERATE INTERMEDIATE RESULT

FIG. 11

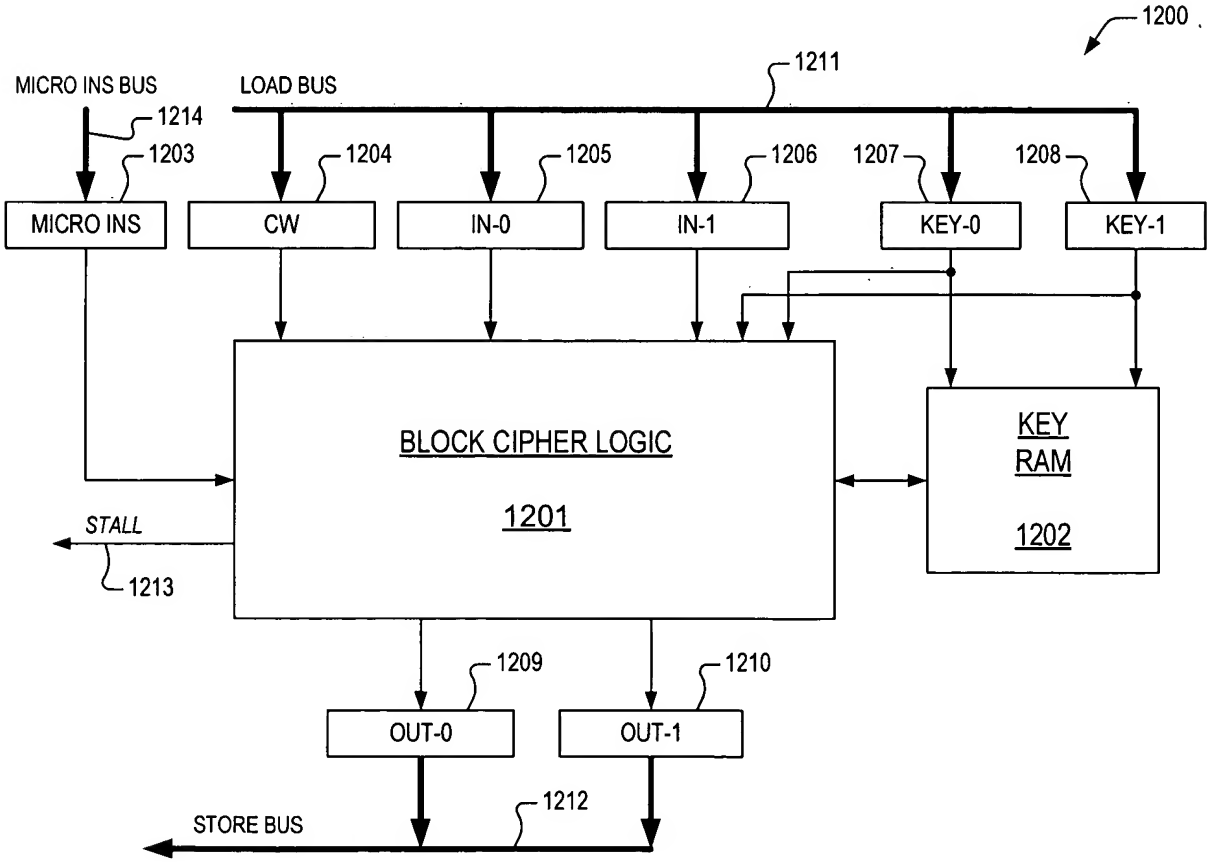

FIG. 12

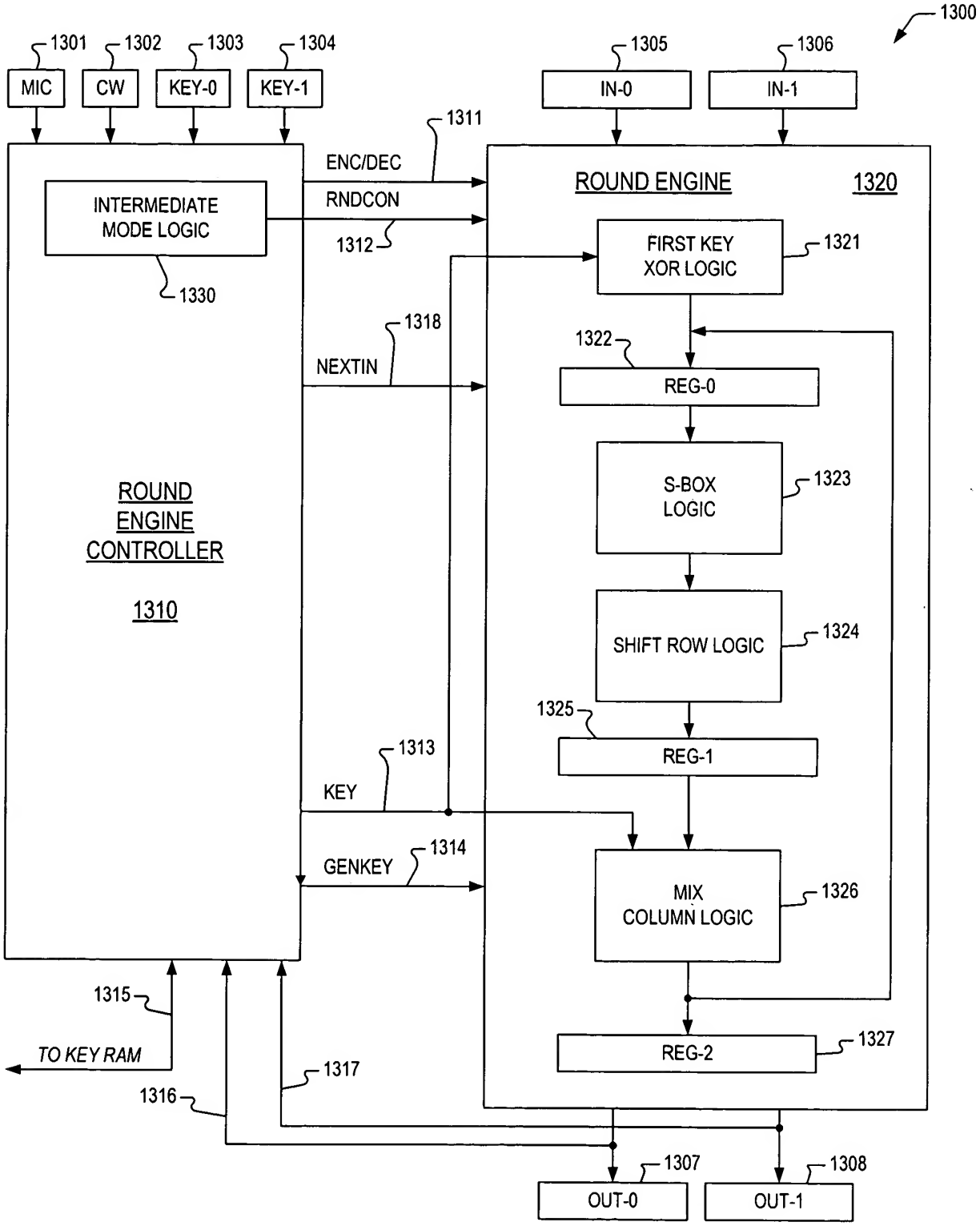
1300
1301
MIC
1302
CW
1303
KEY-0
1304
KEY-1
1305
IN-0
1306
IN-1
1311
ENC/DEC
RNDCON
1312
INTERMEDIATE MODE LOGIC
1330
ROUND ENGINE
1320
FIRST KEY XOR LOGIC
1321
1322
REG-0
1318
NEXTIN
S-BOX LOGIC
1323
SHIFT ROW LOGIC
1324
1325
REG-1
ROUND ENGINE CONTROLLER
1310
1313
KEY
1314
GENKEY
MIX COLUMN LOGIC
1326
1315
TO KEY RAM
1317
REG-2
1327
1316
1307
OUT-0
1308
OUT-1

FIG. 13

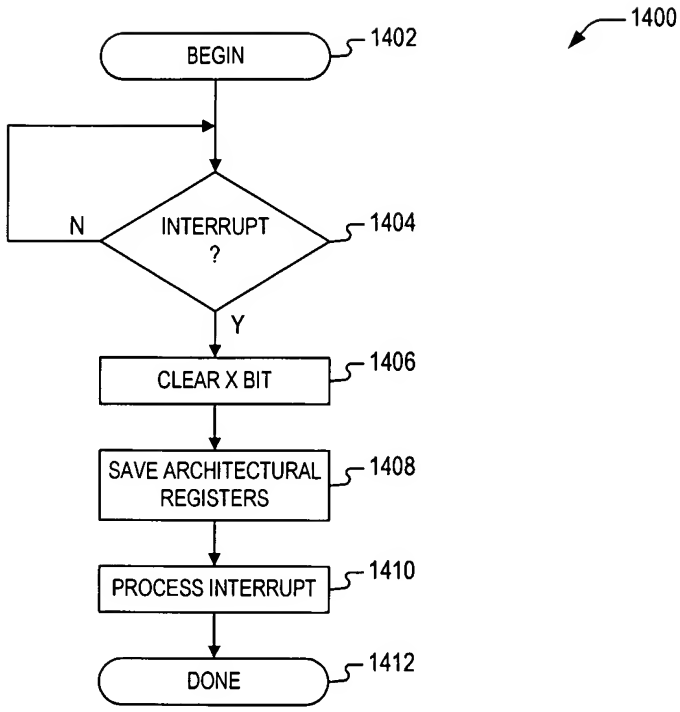
1400
BEGIN
1402
INTERRUPT ?
1404
N
Y
CLEAR X BIT
1406
SAVE ARCHITECTURAL REGISTERS
1408
PROCESS INTERRUPT
1410
DONE
1412

FIG. 14

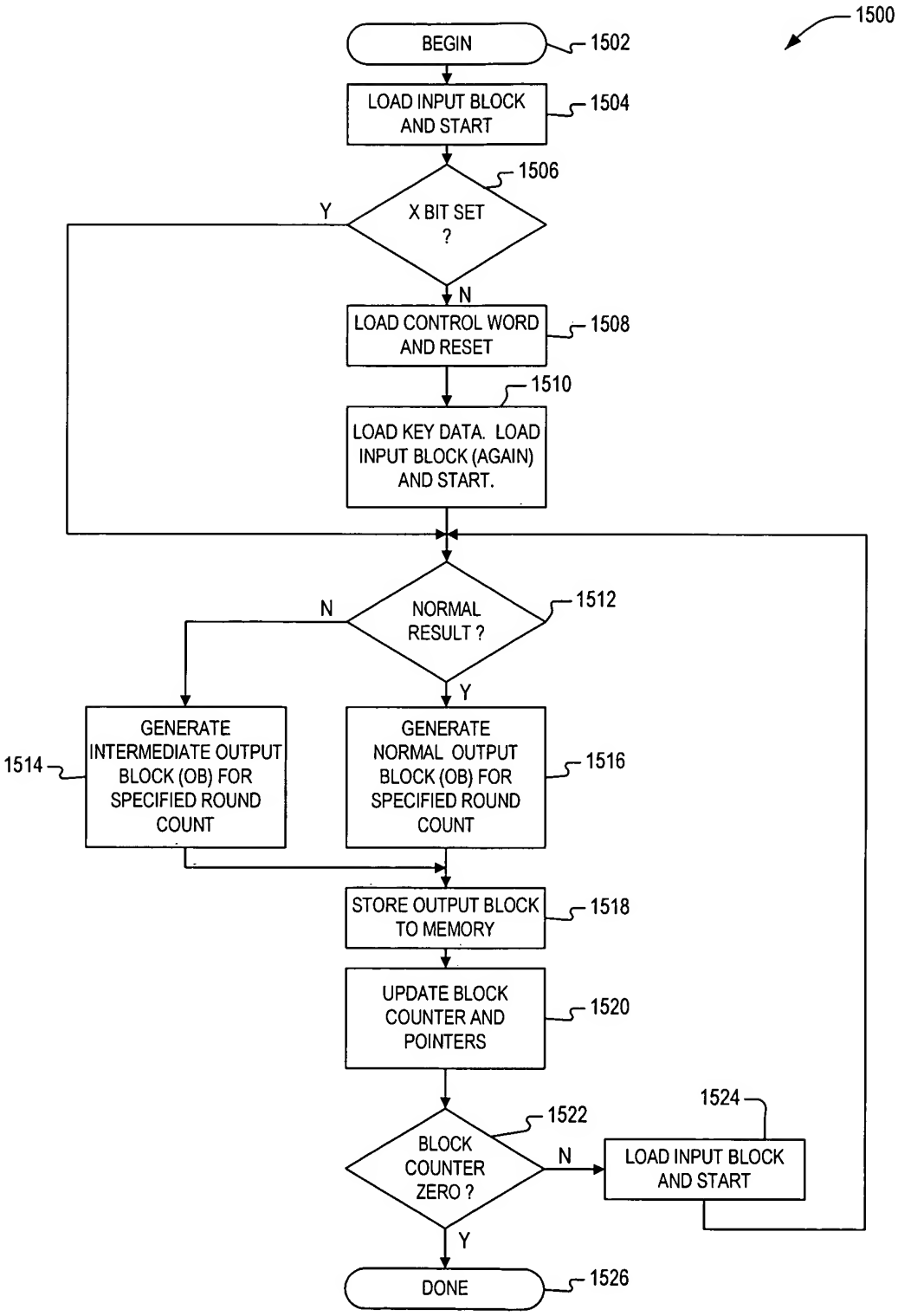
1500
BEGIN
1502
LOAD INPUT BLOCK AND START
1504
1506
X BIT SET ?
Y
N
LOAD CONTROL WORD AND RESET
1508
1510
LOAD KEY DATA. LOAD INPUT BLOCK (AGAIN) AND START.
NORMAL RESULT ?
1512
N
Y
GENERATE INTERMEDIATE OUTPUT BLOCK (OB) FOR SPECIFIED ROUND COUNT
1514
GENERATE NORMAL OUTPUT BLOCK (OB) FOR SPECIFIED ROUND COUNT
1516
STORE OUTPUT BLOCK TO MEMORY
1518
UPDATE BLOCK COUNTER AND POINTERS
1520
1522
BLOCK COUNTER ZERO ?
N
1524
LOAD INPUT BLOCK AND START
Y
DONE
1526

FIG. 15